IDEA GROUP PUBLISHING **ITB13044**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter XI

The Relationship Between Digital Forensics, Corporate Governance, IT Governance and IS Governance

SH (Basie) von Solms, University of Johannesburg, South Africa

CP (Buks) Louwrens, University of Johannesburg, South Africa

Abstract

The purpose of this chapter is twofold: Firstly, we want to determine the relationships, if any, between the discipline of digital forensics and the peer disciplines of corporate governance, information technology governance, and information security governance. Secondly, after we have determined such relationships between these disciplines, we want to determine if there is an overlap between these disciplines, and if so, investigate the content of the overlap between information technology governance and digital forensics.Therefore, we want to position the discipline of digital forensics in relation to corporate governance, information technology governance, and information security governance, and describe in detail the relationship between information technology governance and digital forensics.

Introduction

It is widely accepted today that the increasing and ubiquitous use of computers and Information Technology (IT)-based systems, in all spheres of life, and specifically in the corporate world, had led to companies becoming more and more dependent on their IT systems. Such systems, with all the corporate data and information stored in such systems, had become strategically important for the success or failure of the company.

This increasing use of and dependence on IT systems, had of course created other risks —such as risks of unauthorized access to and use of corporate electronic resources (software, data, and information) which could again result in major problems for the company, including computer crime and fraud.

The challenge to companies therefore is to put measures and processes in place to ensure that the confidentiality, integrity, and availability of all electronic resources are protected, and to ensure that any such crime and fraud are prevented, or when they are committed, to be able to identify and prosecute the culprits.

Two very important disciplines resulted from this challenge. The first is that of information security, which can seen as the discipline to protect the confidentiality, integrity, and availability of all electronic resources, and the other is digital forensics which can be seen as the discipline to ensure that if a crime, involving the confidentiality, integrity, and/or availability of these electronic resources had been committed, the culprits can be identified and prosecuted.

Even from these high-level definitions of information security and digital forensics, it is already intuitively clear that some relationship exists between these two disciplines.

However, information security is a component of information technology (IT) governance, which in itself is again a component of corporate governance.

If a relationship does exist between information security and digital forensics as claimed above, and information security is related to IT and corporate governance, it seems logical that some relationship must also exist between digital forensics, IT governance, and corporate governance.

For any company who wants to create an effective digital forensics environment, it seems prudent to precisely know the relationships between digital forensics, information security, IT governance, and corporate governance. The reason is that if a digital forensics environment is created, and any of the relationships mentioned above are ignored, it may result in an environment which will not operate optimally.

Imagine for example that a digital forensics environment is created with no interface to an existing information security environment in the company. A lot of duplication will result, including the creation of policies and procedures overlapping with information security policies and procedures. A prime example is the backup and archiving of data and information. This is essential for digital forensics, but is most probably already included in the policies and procedures existing within the information security environment. It is therefore important for the company to take this relationship into account to avoid duplication and inconsistencies.